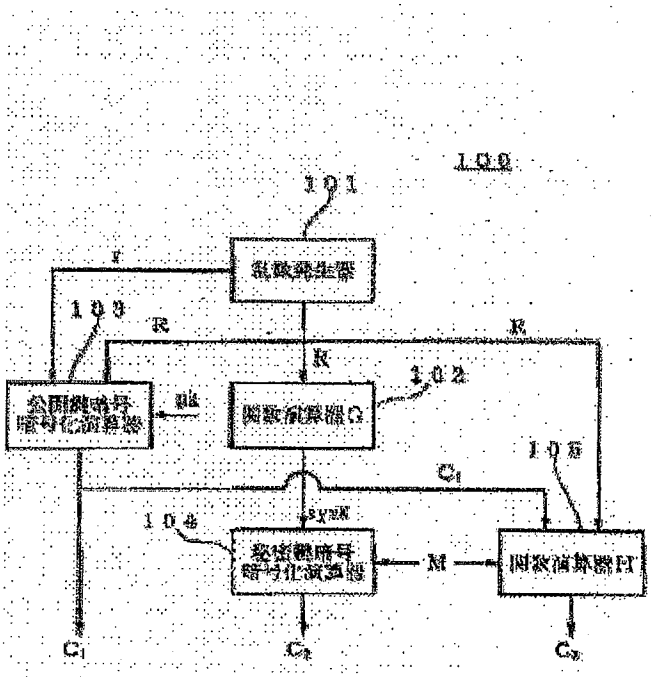
DEVICE AND METHOD FOR CIPHERING, DEVICE AND METHOD FOR DECIPHERING, CIPHER SYSTEM AND RECORDING MEDIUM WHICH STORES THE PROGRAM

Publication number: JP2001222218
Publication date: 2001-08-17
Inventor: OKAMOTO TATSUAKI; DAVID POANSHEBARU
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***G09C1/00;*** **G09C1/00;** (IPC1-7): G09C1/00
- European:
Application number: JP20000032461 20000209
Priority number(s): JP20000032461 20000209

Report a data error here

Abstract of **JP2001222218**

PROBLEM TO BE SOLVED: To obtain a high degree of safety against an active attack with respect to a ciphered sentence by a public key ciphering. SOLUTION: In a ciphering device 100, M is a plain sentence having (t) bits and a random number generator 101 generates a (k) bit random number R and a one bit random number (r). A function computer G102 computes a secret key symK=G(R) by using the number R. Moreover, a ciphered sentence C1=Epk (R, r) is generated by a public key cipher ciphering computer 103 by using the numbers R and (r) and a public key pk. Furthermore, by using the key symK and the sentence M, a ciphered sentence C2=symEsymk(M) is generated by a secret key cipher ciphering computer 104. Then, a function computer H105 computes C3=H (C1, R, M) and C=(C1, C2, C3) is outputted as a ciphered sentence.



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－222218
（P2001－222218A）
(43)公開日　平成13年８月17日(2001.8.17)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード*(参考)
Ｇ０９Ｃ　1/00	６２０	Ｃ０９Ｃ　1/00	６２０Ｚ　５Ｊ１０４

審査請求　未請求　請求項の数13　ＯＬ　（全６頁）

(21)出願番号　特願2000－32461(P2000－32461)

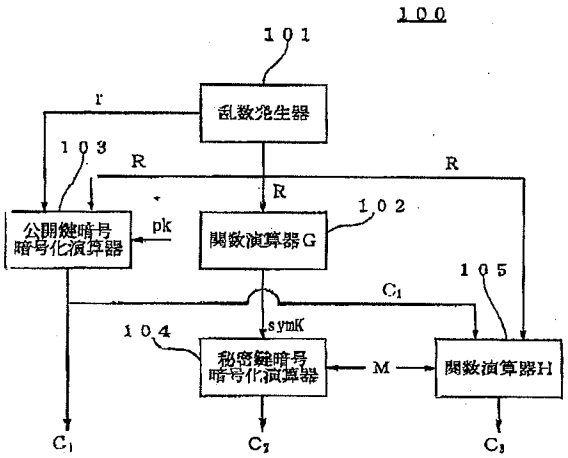
(22)出願日　平成12年２月９日(2000.2.9)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　岡本　龍明
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　ダビド　ポアンシェバル
フランス・75230・パリ・セドゥ・05・ル・ダルム・45
(74)代理人　100064908
弁理士　志賀　正武

Ｆターム(参考)　5J104 JA21 JA30 JA31 NA02

(54)【発明の名称】　暗号化装置、方法、復号装置、方法、暗号システム及びプログラムを記憶した記憶媒体

(57)【要約】
【課題】　公開鍵暗号による暗号文に対する能動的な攻撃に対して高い安全性が得られるようにする。
【解決手段】　暗号化装置１００において、ｔビットの平文をＭとし、乱数発生器１０１よりｋビットの乱数Ｒ及びｌビットの乱数ｒを発生させる。関数演算器Ｇ１０２によりＲを用いて秘密鍵ｓｙｍＫ＝Ｇ（Ｒ）を計算する。また、公開鍵暗号暗号化演算器１０３により、Ｒ，ｒと公開鍵ｐｋとを用いて暗号文$C_1 = E_{pk}(R, r)$を生成する。また、秘密鍵暗号暗号化演算器１０４により、上記秘密鍵ｓｙｍＫと平文Ｍとを用いて暗号文$C_2 = symE_{symK}(M)$を生成する。さらに、関数演算器Ｈ１０５により$C_3 = H(C_1, R, M)$を計算し、$C = (C_1, C_2, C_3)$を暗号文として出力する。



【特許請求の範囲】

【請求項１】 乱数Ｒ，ｒを発生する乱数発生手段と、上記乱数Ｒ，ｒと公開鍵ｐｋとを用いて暗号文C_1＝E_{pk}（Ｒ，ｒ）を計算する公開鍵暗号暗号化演算手段と、上記乱数Ｒと関数Ｇとを用いて秘密鍵ｓｙｍＫ＝Ｇ（Ｒ）を計算する第１の関数演算手段と、

上記秘密鍵ｓｙｍＫと平文Ｍとを用いて暗号文C_2＝$symE_{symK}$（Ｍ）を計算する秘密鍵暗号暗号化演算手段と、

上記乱数Ｒと上記暗号文C_1と上記平文Ｍと関数Ｈとを用いて暗号文C_3＝Ｈ（C_1，Ｒ，Ｍ）を計算する第２の関数演算手段と、

暗号文Ｃ＝（C_1，C_2，C_3）を出力する出力手段とを設けたことを特徴とする暗号化装置。

【請求項２】 上記関数Ｈを任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数Ｇをｋビットのデータをｓビットに変換するランダム関数とすることを特徴とする請求項１記載の暗号化装置。

【請求項３】 乱数Ｒ，ｒと公開鍵ｐｋとを用いて計算された暗号文C_1＝E_{pk}（Ｒ，ｒ）と、上記乱数Ｒと関数Ｇとを用いて計算された秘密鍵ｓｙｍＫ＝Ｇ（Ｒ）と平文Ｍとから計算された暗号文C_2＝$symE_{symK}$（Ｍ）と、上記乱数Ｒと上記暗号文C_1と関数Ｈとを用いて計算された暗号文C_3＝Ｈ（C_1，Ｒ，Ｍ）とからなる暗号文Ｃ＝（C_1，C_2，C_3）を入力する入力手段と、

上記暗号文C_1と秘密鍵ｓｋとを用いて乱数Ｒ′＝D_{sk}（C_1）を計算する公開鍵暗号復号演算手段と、

上記乱数Ｒ′と上記関数Ｇとを用いて秘密鍵ｓｙｍＫ′＝Ｇ（Ｒ′）を計算する第１の関数演算手段と、

上記秘密鍵ｓｙｍＫ′と上記暗号文C_2とを用いて平文Ｍ′＝$symD_{symK}$′（C_2）を計算する秘密鍵暗号復号演算手段と、

上記平文Ｍ′と上記暗号文C_1と上記乱数Ｒ′と上記関数Ｈとを用いて暗号文C_3′＝Ｈ（C_1，Ｒ′，Ｍ′）を計算する第２の関数演算手段と、

上記暗号文C_3′と上記暗号文C_3とを比較する比較手段とを設けたことを特徴とする復号装置。

【請求項４】 上記関数Ｈを任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数Ｇをｋビットのデータをｓビットに変換するランダム関数とすることを特徴とする請求項３記載の復号装置。

【請求項５】 乱数Ｒ，ｒを発生する乱数発生手段と、上記乱数Ｒ，ｒと公開鍵ｐｋとを用いて暗号文C_1＝E_{pk}（Ｒ，ｒ）を計算する公開鍵暗号暗号化演算手段と、上記乱数Ｒと関数Ｇとを用いて秘密鍵ｓｙｍＫ＝Ｇ（Ｒ）を計算する第１の関数演算手段と、

上記秘密鍵ｓｙｍＫと平文Ｍとを用いて暗号文C_2＝$symE_{symK}$（Ｍ）を計算する秘密鍵暗号暗号化演算手段と、

上記乱数Ｒと上記暗号文C_1と上記平文Ｍと上記関数Ｈとを用いて暗号文C_3＝Ｈ（C_1，Ｒ，Ｍ）を計算する第２の関数演算手段と、

暗号文Ｃ＝（C_1，C_2，C_3）を出力する出力手段とを有する暗号化装置と、

上記暗号文Ｃ＝（C_1，C_2，C_3）を入力する入力手段と、

上記暗号文C_1と秘密鍵ｓｋとを用いて乱数Ｒ′＝D_{sk}（C_1）を計算する公開鍵暗号復号演算手段と、

上記乱数Ｒ′と上記関数Ｇとを用いて秘密鍵ｓｙｍＫ′＝Ｇ（Ｒ′）を計算する第３の関数演算手段と、

上記秘密鍵ｓｙｍＫ′と上記暗号文C_2とを用いて平文Ｍ′＝$symD_{symK}$′（C_2）を計算する秘密鍵暗号復号演算手段と、

上記平文Ｍ′と上記暗号文C_1と乱数Ｒ′と上記関数Ｈとを用いて暗号文C_3′＝Ｈ（C_1，Ｒ′，Ｍ′）を計算する第４の関数演算手段と、

上記暗号文C_3′と上記暗号文C_3とを比較する比較手段とを有する復号装置とを備えたことを特徴とする暗号システム。

【請求項６】 上記関数Ｈを任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数Ｇをｋビットのデータをｓビットに変換するランダム関数とすることを特徴とする請求項５記載の暗号システム。

【請求項７】 ｍを平文（暗号の対象となる文書）、ｒを乱数、（ｐｋ，ｓｋ）を公開鍵と秘密鍵の対とするとき、ｐｋ，ｍ，ｒより暗号文Ｃ＝E_{pk}（ｍ，ｒ）が作られるような公開鍵暗号、ならびに秘密鍵ｓｙｍＫと平文ｓｙｍＭとから暗号文ｓｙｍＣ＝$symE_{symK}$（ｓｙｍＭ）が作られ、上記秘密鍵ｓｙｍＫと暗号文ｓｙｍＣとから平文ｓｙｍＭ＝$symD_{symK}$（ｓｙｍＣ）が作られるような秘密鍵暗号を用いて暗号文を生成する暗号化方法であって、

ＨおよびＧを関数とし、

暗号化処理として、平文Ｍと乱数Ｒ及びｒ、公開鍵ｐｋを用いてC_1＝E_{pk}（Ｒ，ｒ），C_2＝$symE_{G(R)}$（Ｍ）及びC_3＝Ｈ（C_1，Ｒ，Ｍ）を生成しＣ＝（C_1，C_2，C_3）を暗号文とすることを特徴とする暗号化方法。

【請求項８】 上記関数Ｈを任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数Ｇをｋビットのデータをｓビットに変換するランダム関数とすることを特徴とする請求項７記載の暗号化方法。

【請求項９】 ｍを平文（暗号の対象となる文書）、ｒを乱数、（ｐｋ，ｓｋ）を公開鍵と秘密鍵の対とするとき、ｐｋ，ｍ，ｒより暗号文Ｃ＝E_{pk}（ｍ，ｒ）が作ら

れるような公開鍵暗号、ならびに秘密鍵ｓｙｍKと平文ｓｙｍMとから暗号文ｓｙｍC＝ｓｙｍE_{symK}（ｓｙｍM）が作られ、上記秘密鍵ｓｙｍKと暗号文ｓｙｍCとから平文ｓｙｍM＝ｓｙｍD_{symK}（ｓｙｍC）が作られるような秘密鍵暗号を用いて生成された暗号文であって、

HおよびGを関数とし、

暗号化処理として、平文Mと乱数R及びｒ、公開鍵ｐｋを用いてC_1＝E_{pk}（R，ｒ），C_2＝ｓｙｍ$E_{G(R)}$（M）及びC_3＝H（C_1，R，M）を生成しC＝（C_1，C_2，C_3）で表される暗号文を復号する復号方法において、

C及び秘密鍵ｓｋ，公開鍵ｐｋよりR′＝D_{sk}（C_1）及びM′＝ｓｙｍ$D_{G(R')}$（C_2）を計算しC_3′＝H（C_1，R′，M′）とC_3とが一致するか否かを検証し、一致すれば、M′を平文Mとして出力することを特徴とする復号方法。

【請求項１０】　上記関数Hを任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数Gをｋビットのデータをｓビットに変換するランダム関数とすることを特徴とする請求項９記載の復号方法。

【請求項１１】　乱数R，ｒを発生する乱数発生手順と、

上記乱数R，ｒと公開鍵ｐｋとを用いて暗号文C_1＝E_{pk}（R，ｒ）を計算する公開鍵暗号暗号化演算手処理と、

上記乱数Rとランダム関数Gとを用いて秘密鍵ｓｙｍK＝G（R）を計算する第１の関数演算手順と、

上記秘密鍵ｓｙｍKと平文Mとを用いて暗号文C_2＝ｓｙｍE_{symK}（M）を計算する秘密鍵暗号暗号化演算手順と、

上記乱数Rと上記暗号文C_1と上記平文Mと関数Hとを用いて暗号文C_3＝H（C_1，R，M）を計算する第２の関数演算手順と、

暗号文C＝（C_1，C_2，C_3）を出力する出力手順とを実行するためのプログラムを記憶した記憶媒体。

【請求項１２】　乱数R，ｒと公開鍵ｐｋとを用いて計算された暗号文C_1＝E_{pk}（R，ｒ）と、上記乱数Rと関数Gとを用いて計算された秘密鍵ｓｙｍK＝G（R）と平文Mとから計算された暗号文C_2＝ｓｙｍE_{symK}（M）と、上記乱数Rと上記暗号文C_1と関数Hとを用いて計算された暗号文C_3＝H（C_1，R，M）とからなる暗号文C＝（C_1，C_2，C_3）を入力する入力処理と、

上記暗号文C_1と秘密鍵ｓｋとを用いて乱数R′＝D_{sk}（C_1）を計算する公開鍵暗号復号演算手順と、

上記乱数R′と上記関数Gとを用いて秘密鍵ｓｙｍK′＝G（R′）を計算する第１の関数演算手順と、

上記秘密鍵ｓｙｍK′と上記暗号文C_2とを用いて平文M′＝ｓｙｍD_{symK}′（C_2）を計算する秘密鍵暗号復号演算手順と、

上記平文M′と上記暗号文C_1と上記乱数R′と関数Hとを用いて暗号文C_3′＝H（C_1，R′，M′）を計算する第２の関数演算手順と、

上記暗号文C_3′と上記暗号文C_3とを比較する比較手順とを実行するためのプログラムを記憶した記憶媒体。

【請求項１３】　上記関数Hを任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数Gをｋビットのデータをｓビットに変換するランダム関数とすることを特徴とする請求項１１又は１２記載のプログラムを記憶した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、文書を公開鍵暗号を用いた暗号文に変換する暗号化装置、方法、暗号文を解読する復号装置、方法、暗号化装置と復号装置からなる暗号システム、及び暗号化装置、復号装置で用いられるプログラムを記憶した記憶媒体に関するものである。

【０００２】

【従来の技術】一般に、暗号法は共通鍵暗号システムと公開鍵暗号システムの二種類に大別できる。公開鍵暗号システムは、共通鍵暗号システムで問題となる鍵配送の問題や鍵の管理の問題などを解決する方法である。代表的な公開鍵暗号として、RSA 暗号、Rabin暗号、ElGamal 暗号、楕円曲線暗号（楕円ElGamal 暗号）などが挙げられる。

【０００３】これらの公開鍵暗号のうちElGamal 暗号、楕円曲線暗号（楕円ElGamal 暗号）などは、暗号化処理に乱数が使われ、確率暗号と呼ばれる。

【０００４】暗号文に対する攻撃法には、大きく分けて受動的攻撃と能動的攻撃とがある。受動的攻撃とは、攻撃者が単に暗号文と公開情報から平文を探索することである。能動的攻撃とは、攻撃者は自分が自由に選択した暗号文を正規の受信者に復号してもらうことができる。能動的攻撃に対しても安全な暗号方式を用いることは、より強い安全性を保証する暗号文を構成することを意味する。

【０００５】従来、RSA 暗号のような確定的な暗号に基づき、能動的攻撃に強い暗号文を作成する一般的な方法としては、Bellare , Rogaway によるOAEP（Optimal Asymmetric Encryption Padding ）という方法が知られている（M. Bellare and P. Rogaway, “Optimal Asymmetric Encryption —How to encrypt with RSA” Advances in Cryptology -EUROCRYPT' 94, LNCS, Springer - Verlag,1995.）。この方法は、ランダム関数（例えば、SHA などのハッシュ関数であり、その具体的な構成法は上記論文に掲載）を２種類用いて構成する方法である。

【０００６】

【発明が解決しようとする課題】しかしながら、上記OA

EPは確率暗号には適用できないため、確率暗号を用いて能動的攻撃に強い暗号文を作成するための一般的な方法は知られていなかった。

【0007】本発明は、一般的な公開鍵暗号（確率暗号を含む）を用いて能動的攻撃に強い暗号文を作成することができるようにすることを目的としている。

【0008】

【課題を解決するための手段】上記の目的を達成するために、本発明による暗号化装置は、乱数R，rを発生する乱数発生手段（例えば実施の形態における乱数発生器101）と、上記乱数R，rと公開鍵pkとを用いて暗号文$C_1=E_{pk}$（R，r）を計算する公開鍵暗号暗号化演算手段（同公開鍵暗号暗号化演算器103）と、上記乱数Rと関数Gとを用いて秘密鍵symK=G（R）を計算する第1の関数演算手段（同関数演算器G102）と、上記秘密鍵symKと平文Mとを用いて暗号文$C_2=symE_{symK}$（M）を計算する秘密鍵暗号暗号化演算手段（同秘密鍵暗号暗号化演算器104）と、上記乱数Rと上記暗号文C_1と上記平文Mと関数Hとを用いて暗号文$C_3=H(C_1, R, M)$を計算する第2の関数演算手段（同関数演算器H105）と、暗号文$C=(C_1, C_2, C_3)$を出力する出力手段とを設けている。

【0009】本発明による復号装置は、上記暗号化装置で生成された上記暗号文$C=(C_1, C_2, C_3)$を入力する入力手段と、上記暗号文C_1と秘密鍵skとを用いて乱数$R'=D_{sk}(C_1)$を計算する公開鍵暗号復号演算手段（同公開鍵暗号復号演算器201）と、上記乱数R′と上記関数Gとを用いて秘密鍵symK′=G（R′）を計算する第1の関数演算手段（同関数演算器G202）と、上記秘密鍵symK′と上記暗号文C_2とを用いて平文$M'=symD_{symK'}(C_2)$を計算する秘密鍵暗号復号演算手段（同秘密鍵暗号復号演算器203）と、上記平文M′と上記暗号文C_2と乱数R′と関数Hとを用いて暗号文$C_3'=H(C_1, R', M')$を計算する第2の関数演算手段（同関数演算器H204）と、上記暗号文C_3'と暗号文C_3とを比較する比較手段（同比較器205）とを設けている。

【0010】本発明による暗号システムは、乱数R，rを発生する乱数発生手段と、上記乱数R，rと公開鍵pkとを用いて暗号文$C_1=E_{pk}$（R，r）を計算する公開鍵暗号暗号化演算手段と、上記乱数Rと関数Gとを用いて秘密鍵symK=G（R）を計算する第1の関数演算手段と、上記秘密鍵symKと平文Mとを用いて暗号文$C_2=symE_{symK}$（M）を計算する秘密鍵暗号暗号化演算手段と、上記乱数Rと上記暗号文C_1と上記平文Mと関数Hとを用いて暗号文$C_3=H(C_1, R, M)$を計算する第2の関数演算手段と、暗号文$C=(C_1, C_2, C_3)$を出力する出力手段とを有する暗号化装置と、上記暗号文$C=(C_1, C_2, C_3)$を入力する入力手段と、上記暗号文C_1と秘密鍵skとを用いて乱数$R'=D_{sk}(C_1)$を計算する公開鍵暗号復号演算手段と、上記乱数R′と上記関数Gとを用いて秘密鍵symK′=G（R′）を計算する第3の関数演算手段（同関数演算器G202）と、上記秘密鍵symK′と上記暗号文C_2とを用いて平文$M'=symD_{symK'}(C_2)$を計算する秘密鍵暗号復号演算手段と、上記平文M′と上記暗号文C_1と乱数R′と関数Hとを用いて暗号文$C_3'=H(C_1, R', M')$を計算する第4の関数演算手段（同関数演算器H204）と、上記暗号文C_3'と暗号文C_3とを比較する比較手段とを有する復号装置とを備えている。

【0011】本発明による暗号方法は、mを平文（暗号の対象となる文書）、rを乱数、（pk，sk）を公開鍵と秘密鍵の対とするとき、pk，m，rより暗号文$C=E_{pk}$（m，r）が作られるような公開鍵暗号、ならびに秘密鍵symKと平文symMとから暗号文$symC=symE_{symK}$（symM）が作られ、上記秘密鍵symKと暗号文symCとから平文$symM=symD_{symK}$（symC）が作られるような秘密鍵暗号を用いて暗号文を生成する暗号化方法であって、HおよびGを関数とし、暗号化処理として、平文Mと乱数R及びr、公開鍵pkを用いて$C_1=E_{pk}$（R，r），$C_2=symE_{G(R)}$（M）及び$C_3=H(C_1, R, M)$を生成し $C=(C_1, C_2, C_3)$を暗号文とするものである。

【0012】本発明による復号方法は、上記暗号方法により生成された暗号文を復号する場合に、C及び秘密鍵sk，公開鍵pkより$R'=D_{sk}(C_1)$及び$M'=symD_{G(R')}(C_2)$を計算し $C_3'=H(C_1, R', M')$とC_3とが一致するかどうかを検証し、一致すれば、M′を平文Mとして出力するものである。

【0013】本発明によるプログラムを記憶した記憶媒体は、乱数R，rを発生する乱数発生手順と、上記乱数R，rと公開鍵pkとを用いて暗号文$C_1=E_{pk}$（R，r）を計算する公開鍵暗号暗号化演算手処理と、上記乱数Rと関数Gとを用いて秘密鍵symK=G（R）を計算する第1の関数演算手順と、上記秘密鍵symKと平文Mとを用いて暗号文$C_2=symE_{symK}$（M）を計算する秘密鍵暗号暗号化演算手順と、上記乱数Rと上記暗号文C_1と上記平文Mと関数Hとを用いて暗号文$C_3=H(C_1, R, M)$を計算する第2の関数演算手順と、暗号文$C=(C_1, C_2, C_3)$を出力する出力手順とを実行するためのプログラムを記憶したものである。

【0014】本発明による他のプログラムを記憶した記憶媒体は、上記記憶媒体の処理により生成された上記暗号文$C=(C_1, C_2, C_3)$を入力する入力処理と、上記暗号文C_1と秘密鍵skとを用いて乱数$R'=D_{sk}(C_1)$を計算する公開鍵暗号復号化演算手順と、上記乱数R′と上記関数Gとを用いて秘密鍵symK′=G（R′）を計算する第1の関数演算手順と、上記秘密鍵symK′と上記暗号文C_2とを用いて平文$M'=s$

$symD_{symK}'$（C_2）を計算する秘密鍵暗号復号化演算手順と、上記平文M′と上記暗号文C_1と乱数R′と関数Hとを用いて暗号文C_3'＝H（C_1，R′，M′）を計算する第2の関数演算手順と、上記暗号文C_3'と暗号文C_3とを比較する比較手段とを実行するためのプログラムを記憶したものである。

【0015】

【発明の実施の形態】以下、本発明の実施の形態を図面と共に説明する。本実施の形態は、一般的な公開鍵暗号を用いて能動的攻撃に強い暗号文を構成する方法として、ランダム関数を2回利用するだけで所定の安全性が得られる新しい暗号方式を提案するものである。

【0016】図1は本実施の形態による公開鍵暗号を用いた暗号化装置100を示すブロック図、図2は暗号化装置100で作成された暗号文を解読（復号）する復号装置200を示すブロック図である。上記暗号化装置100及び復号装置200により暗号システムが構成される。

【0017】次に、暗号化処理及び復号処理について説明する。まず、ある公開鍵暗号を仮定する。この公開鍵暗号は、mを平文（暗号の対象となる文書）、rを乱数、（pk，sk）を公開鍵と秘密鍵の対とするとき、暗号文cは、$c=E_{pk}(m, r)$で表現する。また、秘密鍵を用いた復号関数は、D_{sk}で表現する。このとき、mの長さをkビット、rの長さを1ビットとする。

【0018】また、ある秘密鍵暗号を仮定する。この秘密鍵暗号では、秘密鍵symKと平文symMから、暗号文$symC=symE_{symK}(symM)$が作られ、また、秘密鍵symKと暗号文symCから平文$symM=symD_{symK}(symC)$が復号される。ここで、symKの長さをsビットとする。

【0019】また、Hを任意のサイズのデータを特定のサイズのデータに変換するランダム関数、Gをkビットのデータをsビットに変換するランダム関数とする（このようなランダム関数の具体例については、上記OAEPの論文を参照）。

【0020】まず、図1の暗号化装置100による暗号化処理について説明する。図1において、tビットの平文をMとする。乱数発生器101よりkビットの乱数Rと1ビットの乱数rを発生させる。そして、関数演算器G102により乱数Rを用いて秘密鍵symK＝G（R）を計算する。

【0021】また、公開鍵暗号暗号化演算器103に上記乱数R，rと公開鍵pkとを入力して暗号文$C_1=E_{pk}(R, r)$を生成する。次に、秘密鍵暗号暗号化演算器104に、上記Mと関数演算器G102で計算された秘密鍵symKとを入力し、暗号文$C_2=symE_{symk}(M)$を生成する。さらに、関数演算器H105に、公開鍵暗号暗号化演算器103で計算された上記暗号文C_1と乱数Rとを入力して、暗号文C_3＝H（C_1，R，M）を計算し、C＝（C_1，C_2，C_3）を暗号文として出力する。

【0022】次に、図2の復号装置200による復号処理について説明する。図2において、復号装置200には、暗号化装置100で生成された暗号文C＝（C_1，C_2，C_3）が入力される。公開鍵暗号復号演算器201は、秘密鍵skとC_1とから乱数$R'=D_{sk}(C_1)$を計算する。次に、関数演算器G202により上記R′を用いて秘密鍵$symK'=G(R')$を計算する。次に、秘密鍵暗号復号演算器203は、上記秘密鍵symK′とC_2から平文$M'=symD_{symK'}(C_2)$を計算する。

【0023】次に、関数演算器H204により上記C_1，R′，M′より暗号文C_3'＝H（C_1，R′，M′）を計算する。次に、比較器205により、上記C_3'の値と暗号化装置100から入力されたC_3の値とが等しいか否かを検証する。そして、もし等しくなければ、何も出力しない（もしくは、「検証不合格（NG）」を出力する）。もし等しければ（OKなら）、上記M′を元の平文Mとして出力する。

【0024】このように本実施の形態によれば、ランダム関数G，Hを用いることにより、暗号文Cを復号する者は、送信者が暗号文Cの復号結果である平文Mの値を知っていたかどうかを検証できる。従って、復号処理の検証に合格した場合は、送信者が暗号文Cの復号結果である平文Mの値を知っていたことを確認できるため、能動的攻撃に対しても安全性を保証することができる。

【0025】さらに、秘密鍵暗号（$symE_{symK}$，$symD_{symK}$）及び関数G，Hの演算量が、公開鍵暗号（E_{pk}，D_{sk}）の演算量に比べて小さいと仮定すると、本実施の形態による暗号方式の演算量は、元の公開鍵暗号（E_{pk}，D_{sk}）の演算量とほぼ同等である。即ち、本実施の形態により処理量のオーバーヘッドをほぼ無くしながら、安全性を向上させることが可能である。

【0026】尚、本実施の形態による暗号化装置100及び復号装置200において、前述した暗号化処理及び復号処理をそれぞれコンピュータシステムで実行する場合、そのコンピュータシステムにおけるCPUが実行するプログラムを記憶した記憶装置は、本発明によるプログラムを記憶した記憶媒体を構成する。この記憶媒体としては、各種のディスク媒体や半導体メモリ、磁気記録媒体等を用いることができる。

【0027】

【発明の効果】以上説明したように本発明によれば、暗号文に対する能動的な攻撃に対して高い安全性を保証することができ、かつ少ない演算量で高い安全性を保証することができる。

【図面の簡単な説明】

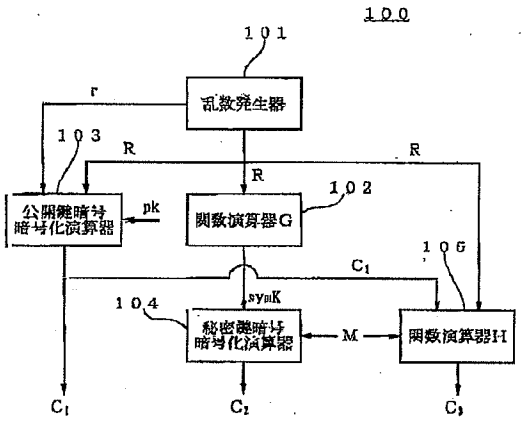
【図1】 本発明の実施の形態による暗号化装置100の構成を示すブロック図である。

【図２】　本発明の実施の形態による復号装置２００の構成を示すブロック図である。

【符号の説明】

１００　暗号化装置
１０１　乱数発生器
１０２　関数演算器Ｇ
１０３　公開鍵暗号暗号化演算器
１０４　秘密鍵暗号暗号化演算器
１０５　関数演算器Ｈ
Ｒ，ｒ　乱数
ｓｙｍＫ　秘密鍵
C_1，C_2，C_3　暗号文
Ｍ　平文
２００　復号装置
２０１　公開鍵暗号復号演算器
２０２　関数演算器Ｇ
２０３　秘密鍵暗号復号演算器
２０４　関数演算器Ｈ
２０５　比較器
ｓｋ　秘密鍵
Ｒ′　乱数
ｓｙｍｋ′　秘密鍵
C_3′　暗号文
Ｍ′　平文

【図１】



【図２】